UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/085,895	02/28/2002	Ted Christian Johnson	10017900-1	2863

7590   08/21/2007

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER
PEARSON, DAVID J

ART UNIT	PAPER NUMBER
2137	

MAIL DATE	DELIVERY MODE
08/21/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

PTOL-90A (Rev. 04/07)

	Application No.	Applicant(s)
Office Action Summary	10/085,895	JOHNSON, TED CHRISTIAN
	Examiner	Art Unit	
	David J. Pearson	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on <u>04 May 2007</u>.

2a) ☐ This action is **FINAL**.   2b) ☒ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) *1-28* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) *1-28* is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☐ All   b) ☐ Some * c) ☐ None of:

      1. ☐ Certified copies of the priority documents have been received.

      2. ☐ Certified copies of the priority documents have been received in Application No. _____.

      3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

1.   Claims 1-28 have been examined.

Response to Arguments

2.   In view of the Appeal Brief filed on 05/04/2007, PROSECUTION IS HEREBY

REOPENED. New grounds of rejection are set forth below.

· To avoid abandonment of the application, appellant must.exercise one of the

following two options:

        (1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply

under 37 CFR 1.113 (if this Office action is final); or,

        (2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed

by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and

appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth

in 37 CFR 41.20 have been increased since they were previously paid, then appellant

must pay the difference between the increased fees and the amount previously paid.

        A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by

signing below:

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of
matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the
conditions and requirements of this title.

3.   Claims 17-20 are rejected under 35 U.S.C. 101 because the claimed invention is

directed to non-statutory subject matter.

Claims 17-20 are directed towards a system. However the elements of the

"system" are logic. At best, logic configured to perform steps is computer program, per

se and can be considered functional descriptive material. Note MPEP 2106.01 for

guidance on computer related non-statutory subject matter.

Claim Rejections - 35 USC § 103

The text of those sections of Title 35, U.S. Code not included in this action can

be found in a prior Office action.

4.   Claims 1-2, 4-5, 8-13 and 17-24 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Reiche (U.S. Patent 6,092,196), and further in view of Brothers (U.S.

Patent Application Publication 2002/0083178).

For claim 1, Reiche teaches a method for authenticating a web session

comprising:

receiving a user ID (note column 10, lines 5-7);

computing a message digest of the user ID (note column 10, lines 19-20 and

column 12, line 24);

computing an expiration timestamp for the session (note column 10, lines 14-15);

combining the message digest and expiration timestamp (note column 10, lines

19-20);

encrypting a message using an encryption key (note column 10, lines 21-23);

and

converting the encrypted message into an ASCII string (note column 10, lines 23-

24).

Reiche differ from the claimed invention in that they fail to specify:

Selecting an index number;

Accessing an encryption key using the index number;

Brothers teaches:

Selecting an index number (note paragraph [0104]);

Accessing an encryption key using the index number (note paragraph [0104]);

It would have been obvious to one of ordinary skill in the art at the time of the

invention to combine Reiche with the key index of Brothers. The combination of Reiche

and Brothers would teach a system that selected a key using an index number

(Brothers) and used the key to encrypt a URL message (Reiche). One of ordinary skill

in the art at the time of the invention would have been motivated to combine Reiche and

Brothers because it would increase security because using a different key for each

session makes the same log in information appear different for each session, making it more difficult to break the encryption scheme or perform a replay attack.

For claim 17, the combination of Reiche and Brothers teaches a system for authenticating a transaction comprising:

Logic configured to receive a user ID (note column 10, lines 5-7 of Reiche);

Logic configured to compute a message digest of the user ID (note column 10, lines 19-20 and column 12, line 24 of Reiche);

Logic configured to select an index number (note paragraph [0104] of Brothers);

Logic configured to combine the message digest with expiration timestamp (note column 10, lines 14-20 of Reiche);

Logic configured to select an encryption key from a plurality of encryption keys using the index number (note paragraph [0104] of Brothers);

Logic configured to encrypt the combined message using the selected encryption key (note column 10, lines 21-23 of Reiche); and

Logic configured to convert the encrypted message into an ASCII string (note column 10, lines 23-24 of Reiche).

For claim 21, the combination of Reiche and Brothers teaches a method for authenticating a transaction comprising:

Computing a message digest of a user ID (note column 10, lines 19-20 and column 12, line 24 of Reiche);

Concatenating the message digest with an expiration timestamp (note column

10, lines 14-20 of Reiche);

Selecting an index number (note paragraph [0104] of Brothers);

Selecting an encryption key from a plurality of encryption keys using the index

number (note paragraph [0104] of Brothers);

Encrypting the message digest using the selected encryption key (note column

10, lines 21-23 of Reiche); and

Converting the encrypted message into an ASCII string (note column 10, lines

23-24 of Reiche).

For claim 2, the combination of Reiche and Brothers teaches claim 1, wherein

the step of combining the message digest and expiration timestamp more specifically

includes concatenating the message digest and expiration timestamp (note column 10,

lines 19-21 of Reiche).

For claim 4, the combination of Reiche and Brothers teaches claim 1, wherein

the step of receiving the user ID more specifically comprises receiving the user ID

through an HTML page (note column 1, lines 60-65 of Reiche) that is communicated

from a remote client browser (note column 9, lines 27-30 of Reiche).

For claim 5, the combination of Reiche and Brothers teaches claim 1, wherein

the step of computing a message digest of the user ID more specifically comprises

computing a four-byte binary value which is an encoded form the user ID (note column

12, line 24 of Reiche).

For claim 8, the combination of Reiche and Brothers teaches claim 1, wherein

the step of accessing the encryption key more specifically comprises retrieving an

encryption key from a storage segment containing a plurality of encryption keys (note

paragraph [0165] of Brothers), wherein the retrieved encryption key is obtained from a

location or position within the storage segment based upon the index number (note

paragraph [0165] of Brothers).

For claim 9, the combination of Reiche and Brothers teaches claim 1, wherein

the step of encrypting the combined message more specifically comprises encrypting

the combined message digest and timestamp into an eight-byte value (note column 11,

lines 51 and 53).

For claim 10, the combination of Reiche and Brothers teaches claim 1, further

comprising the step of concatenating the index number to the encrypted message (note

paragraph [0165] of Brothers).

For claims 11 and 13, examiner took Official Notice that the encrypted message

is converted into an ASCII string using a "printf" command in Office Actions dated

02/15/2006 and 10/12/2006. Applicant did not traverse examiner's assertion and this statement is taken to be admitted prior art (note MPEP 2144.03).

For claim 12, the combination of Reiche and Brothers teaches claim 1, wherein the step of converting the encrypted message into an ASCII string more specifically includes converting the encrypted message into a hexadecimal value (note column 2, lines 24-26 of Reiche).

For claim 18, the combination of Reiche and Brothers teaches claim 17, further including logic configured to generate an expiration timestamp (note column 10, lines 14-15 of Reiche).

For claim 19, the combination of Reiche and Brothers teaches claim 17, further including logic configured to communicate the ASCII string to a remote computer (note column 10, lines 24-29 of Reiche).

For claim 20, the combination of Reiche and Brothers teaches claim 17, further including a local memory for storing the plurality of encryption keys (note paragraph [0165] of Brothers).

For claim 22, the combination of Reiche and Brothers teaches claim 21, wherein the step of encrypting the message more specifically includes encrypting the

concatenated message (note column 10, lines 21-23 of Reiche) using the accessed

encryption key (note paragraph [0104] of Brothers).

For claim 23, the combination of Reiche and Brothers teaches claim 21, wherein

the step of selecting the encryption key more specifically includes retrieving the

encryption key form a local memory based on the index number (note paragraph [0165]

of Brothers).

For claim 24, the combination of Reiche and Brothers teaches claim 21, further

including the step of communicating the ASCII string to a remote computer (note

column 10, lines 24-29 of Reiche).

5.   Claims 3, 14 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable

over the combination of Reiche and Brothers as applied to claim 1 above, and further in

view of Berners-Lee et al. and Verio.

For claim 3, the combination of Reiche and Brothers teaches claim 1, further

comprising passing the ASCII string to a remote computer within an HTML page (note

column 1, lines 60-65 of Reiche).

The combination of Reiche, Rail, Serbinis et al. and Garrison differ from the

claimed invention in that they fail to specify the ASCII string is passed in an FTP URL

being of the form ftp://ID:ASCII@hostname, wherein ID is the user ID and ASCII is the ASCII string.

Berners-Lee et al. teach "URL schemes that involve the direct use of an IP-based protocol to a specified host on the Internet use a common syntax for the scheme-specific data: //<user>:<password>@<host>:<port>/<url-path>" They go on to specify that <user> and <password> as "user: An optional user name. Some schemes (e.g., ftp) allow the specification of a user name. Password: An optional password. If present, it follows the user name separated from it by a colon." (note section 3.1 on page 5)

The Verio glossary defines password as "A series of characters that enables someone to access a file, computer or program." This definition would make the ASCII value a password because it is a series of characters that are enabling a user to access files on an FTP server.

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the combination of combination of Reiche and Brothers with passing the ASCII value in an FTP URL of Berners-Lee et al. One of ordinary skill in the art at the time of the invention would have been motivated to combine Reiche, Brothers and Berners-Lee et al. because it would provide a convenient way for a user to pass their user ID and password to a FTP server.

For claim 14, the combination of Reiche, Brothers and Berners-Lee et al. teach a method of claim 3, further including the step of passing the index number to the remote computer (note paragraph [0165] of Brothers).

For claim 15, the combination of Reiche, Brothers and Berners-Lee et al. teach a method of claim 14, wherein the step of passing the index number to the remote computer more specifically comprises passing the index number to the remote computer separate from the ASCII string (note paragraph [0019] of Brothers).

6.   Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Reiche and Brothers as applied to claim 1 above, and further in view of Krishnaswamy et al (U.S. Patent 6,909,708).

For claim 6, the combination of Reiche and Brothers differ from claimed invention in that they fail to specify the expiration timestamp is computed in Epoch format.

Krishnaswamy et al. teach a communication method that "records timepoints in the epoch time format." (note column 265, lines 37-46)

It would have been obvious to one of ordinary skill in the art at the time of the invention to form the combination of Reiche and Brothers that computed the timestamp in Epoch format of Krishnaswamy et al. One of ordinary skill in the art at the time of the invention would have been motivated to combine Reiche, Brothers and Krishnaswamy et al. because it would solve the problems associated with converting to and from daylight savings time (note column 265, lines 37-46 of Krishnaswamy et al.).

7.   Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Reiche and Brothers as applied to claim 1 above, and further in view of Tan (U.S. Patent 6,490,353).

For claim 7, the combination of Reiche and Brothers differs from the claimed invention in that they fail to specify the index number used to access the encryption key is randomly generated.

Tan teaches a key management scheme where "it may select these [key start points and lengths] by randomly selecting table entry numbers."

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the combination of Reiche and Brothers with the randomly selected index numbers of Tan. One of ordinary skill in the art at the time of the invention would have motivated to combined Reiche, Brothers and Tan because an unpredictable sequence of encryption keys would decrease the likelihood of breaking the encryption method.

8.   Claim 25 is rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Reiche and Brothers as applied to claim 21 above, and further in view of Swartz et al (U.S. Patent 6,095,418).

For claim 25, the combination of Reiche and Brothers differs from the claimed invention in that it fails to specify including the step of communicating the ASCII string to a person through voice communication.

Swartz et al. teach communicating the ASCII string to a person through voice
communication (note column 4, lines 39-44).

It would have been obvious to one of ordinary skill in the art at the time of the
invention to combine the combination of Reiche and Brothers with the spoken ASCII of
Swartz et al. to form a device which converted the message digest to ASCII and then
read the string aloud to someone. One of ordinary skill in the art at the time of the
invention would have been motivated to combine Reiche, Brothers and Swartz et al.
because it provide a convenient way to give the user their authenticated message
digest when they do not have access to a computer or an Internet connection.

9.   Claims 26-28 rejected under 35 U.S.C. 103(a) as being unpatentable over the
combination of Reiche and Brothers as applied to claim 21 above, and further in view of
Stern (U.S. Patent 6,110,044).

For claims 26-28, the combination of Reiche and Brothers differs from the
claimed invention in that they fail to specify the ASCII string is printed onto a ticket
selected from the group consisting of an airline ticket, a concert ticket, an employee ID
card, and an event ticket and further specifying the ASCII string be printed on the ticket
in a form that it may be later electronically scanned for verification.

Stern teaches a ticket printing and verification method which "contains a barcode
printer (or other means for embodying a machine-readable indicium in a payout ticket),
which prints both alphanumeric and barcode information on a payout ticket, including a
validation number." (note column 3, lines 8-12) Note that in this case, a payout ticket

would be an event ticket because successful verification of the ticket results in a payout

event. Stern also teaches, "Selection circuitry 105 may also contain circuitry for

encrypting all or part of the barcoded data imprinted on the payout ticket." (note column

4, lines 49-51)

It would have been obvious to one of ordinary skill in the art at the time of the

invention to combine the combination of Reiche and Brothers, which printed the ASCII

string on an event ticket with a bar code of Stern. One or ordinary skill in the art at the

time of the invention would have been motivated to combine Reiche, Brothers and Stern

because it would provide a convenient and secure way to produce and verify the

authenticity of a monetary winnings event ticket, which would be ideal for casino or

other gaming companies.

10.   Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over Reiche,

Brothers and Berners-Lee et al. as applied to claim 14 above, and further in view of

Tan.

For claim 16, the combination of Reiche, Brothers and Berners-Lee et al. differs

from the claimed invention in that they fail to specify converting the encrypted message

into an ASCII string more specifically comprises converting a combination of the

encrypted message and the index number into an ASCII string, wherein the index

number is communicated to the remote computer as a part of the ASCII string.

Tan teaches a key management scheme where "the seed (randomly generated

index number) may be communicated as part of the message transmission."

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the combination of Reiche, Brothers and Berners-Lee et al. which includes the index number in the message transmission of Tan. One or ordinary skill in the art at the time of the invention would have been motivated to combine Reiche, Brothers, Berners-Lee et al. and Tan because it would provide a convenient way of storing the index number so the server would not have to locally store which cookie is encrypted with which key.

Conclusion

11.   Any inquiry concerning this communication or earlier communications from the examiner should be directed to David J. Pearson whose telephone number is (571) 272-0711. The examiner can normally be reached on Monday - Friday, 8:00am - 4:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

DJP

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER